

NR:VTN
F. #2017R01361

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
ONE ZTE Z861BL CELLULAR PHONE
BEARING SERIAL NUMBER
329F74220C07

APPLICATION FOR A SEARCH
WARRANT FOR AN ELECTRONIC
DEVICE

Case No. 19-MJ-281

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Christopher Carr, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Amtrak Office of Inspector General's Office of Investigations ("Amtrak OIG"). I have participated in both state and federal fraud investigations and have received extensive training in this area. I have been employed as a federal law enforcement officer since 2014. During the course of these investigations, I have conducted or participated in surveillance, the execution of search warrants, and the review of electronic evidence.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a one ZTE Z861BL cellular phone bearing serial number 329F74220C07 (the “Device”). The Device is currently in the custody of Pretrial Services for the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. Amtrak is a national passenger railroad service. Among the different methods of payment accepted by Amtrak, Amtrak allows customers to redeem eVouchers for travel. An eVoucher is a transferable electronic certificate of credit offered by Amtrak when a customer cancels or changes an existing reservation. A single eVoucher can be broken down into multiple eVouchers of lesser value and used to make multiple reservations for future travel. Multiple eVouchers can also be aggregated and used to pay for a single reservation. To redeem an eVoucher, an Amtrak customer must provide the telephone number or email address that was used to make the original reservation.

7. I am part of a joint investigation involving Amtrak OIG, Amtrak Police Department (“APD”), Homeland Security Investigations (“HSI”), and the Department of Transportation Office of Inspector General to identify those responsible for a scheme involving wire fraud and access device fraud that has resulted in a loss of more than \$450,000 to Amtrak in or about and between April 2016 and July 2018. Individuals participating in the scheme purchased Amtrak reservations using stolen credit card account information, cancelled or exchanged those reservations for eVouchers, and sold the eVouchers on the internet, including on eBay and Craigslist.

8. Amtrak OIG agents identified eVouchers sold on the internet as fraudulent whenever the true owners of the credit card accounts used to make the original Amtrak purchases reported those purchases as unauthorized to their financial institutions. Those financial institutions contacted Amtrak and, in turn, received a refund from Amtrak.

9. Amtrak OIG agents identified four separate eBay accounts, specifically “lipheth715,” “2iladam,” “iminyourhome” and “richjerk” (the “eBay Accounts”), that belong to and were used by LAMONT BROWN, ADAM MICEK, KEVIN NELSON and ANDRE WILBURN, respectively, to sell eVouchers that have been identified as part of the fraudulent scheme described above.

- a. In or about and between June 2017 to June 2018, approximately 213 eVouchers worth more than \$60,000 of Amtrak credit were sold by eBay user “lipheth715.” Approximately 161 of these eVouchers, worth approximately \$46,000, have been confirmed as fraudulent as of August 28, 2018. According to records obtained from eBay, “lipheth715” is an eBay account registered to LAMONT BROWN of Brooklyn, New York.
- b. In or about and between November 2016 and July 2017, approximately 286 eVouchers worth more than \$110,000 of Amtrak credit were sold by eBay user “2iladam.” Approximately 140 of these eVouchers, worth approximately \$55,000, have been confirmed as fraudulent as of August 28, 2018. According to records obtained from eBay, “2iladam” is an eBay account registered to ADAM MICEK of Glendale, New York.
- c. In or about and between April 2016 to July 2018, approximately 281 eVouchers worth more than \$250,000 of Amtrak credit were sold by eBay user “iminyourhome.” Approximately 152 of these eVouchers, worth approximately \$136,000, have been confirmed as fraudulent as of August 28, 2018. According to records obtained from eBay, “iminyourhome” is an eBay account registered to KEVIN NELSON of Queens, New York.
- d. In or about and between April 2016 to May 2016, approximately 42 eVouchers worth more than \$30,000 of Amtrak credit were sold by eBay user “richjerk.” Approximately 17 of these eVouchers, worth approximately \$10,000, have been confirmed as fraudulent as of August 28, 2018. According

to records obtained from eBay, "richjerk" is an eBay account registered to ANDRE WILBURN of New York, New York.

10. Each of the eBay Accounts received payments from buyers of eVouchers via PayPal, which is an online payment system. In order to use PayPal, a user must provide a valid bank account or credit card account to which the PayPal account can be linked.

11. Only a portion of the eVouchers sold by the eBay Accounts was identified as fraudulent by Amtrak using the criteria described in paragraph 8 above. I believe that the remainder of the eVouchers sold by the eBay Accounts were also fraudulent; however Amtrak has not issued refunds in those instances. Based on the investigation to date, I believe that refunds have not been issued because the financial institutions absorbed the loss directly, are still in the process of requesting a refund from Amtrak, or because the true accountholders failed to notice and report the original transactions as unauthorized. The remainder of the eVouchers sales is also believed to be fraudulent because the eVouchers were typically sold by the eBay Accounts at heavily discounted prices of 30 to 70 percent of their face value, which, based on my training and experience, is a practice frequently used by individuals committing access device fraud.

12. During the course of our investigation, law enforcement agents identified financial transactions between LAMONT BROWN and ANDRE WILBURN which reflect that BROWN transferred the proceeds from fraudulent eVoucher sales to WILBURN. From on or about and between October 2017 to March 2018, a Square Cash ("SQC") account in the name of "lifeofdre" received deposits from a SQC account in the name of "bigmont715." SQC is an online payment system. In order to use SQC, a user must provide a valid bank

account or credit card account to which the SQC account can be linked. The “lifeofdre” SQC account is owned by ANDRE WILBURN. The “bigmont715” SQC account is owned by LAMONT BROWN and funded by the bank account owned by LAMONT BROWN which is linked to the PayPal account registered to the “liph715” eBay account.

13. On or about February 15, 2018, an undercover agent posing as a buyer (the “Buyer”) purchased an eVoucher worth \$320 that was offered for sale by eBay user “liph715” for the price of \$240. On or about February 17, 2018, Buyer emailed eBay user “liph715”, stating, in substance, that he was having problems making a reservation on Amtrak’s website using the eVoucher he had purchased. Buyer and eBay user “liph715” exchanged a few more email messages and eBay user “liph715” provided Buyer with a replacement eVoucher. Buyer subsequently asked eBay user “liph715” to call Buyer back. Buyer received a call from phone number (347) 403-6607 on or about February 18, 2018 from a man who identified himself as “Lamont” and apologized for having provided Buyer with an incomplete eVoucher number and assured Buyer that the replacement eVoucher would work.

14. On or about September 6, 2018, law enforcement agents executed a search of the residence of LAMONT BROWN in Brooklyn, New York, pursuant to a warrant ordered by The Honorable Peggy Kuo, Magistrate Judge for the Eastern District of New York (Dkt. 18-MJ-827). The warrant authorized law enforcement agents to seize and search any computer or storage medium for records relating to violations of Title 18, United States Code, Sections 1029 and 1956(a)(1)(B)(i). As a result of the search, law enforcement agents seized a number of electronic devices, including one Samsung Galaxy S7 Edge cellular phone (the “Galaxy S7”) and

one iPhone S cellular phone (the “iPhone S”). A forensic search of the Galaxy S7 and the iPhone S revealed numerous messages exchanged LAMONT BROWN and ANDRE WILBURN about eVoucher sales via Telegram and WhatsApp.¹ Moreover, the iPhone S was identified as having a MSISDN number of 13474036607. An MSISDN number is the telephone number assigned to the SIM card used by a cellular phone. The MSISDN number of the iPhone S corresponds to the phone number that Buyer used in February 2018 to contact eBay user “liph715.”

15. On the same date as the execution of the search warrant of LAMONT BROWN’s residence, law enforcement agents interviewed BROWN. BROWN stated, in sum and substance and in part, that his phone number is (347) 403-6607, that he obtained information about eVouchers to sell on eBay from ANDRE WILBURN, and that he received one-third of the profits from eVoucher sales while WILBURN received two-thirds of the profits.

16. Warrants for the arrests of LAMONT BROWN, ADAM MICEK, KEVIN NELSON and ANDRE WILBURN were ordered by The Honorable Steven M. Gold, Magistrate Judge for the Eastern District of New York, on February 15, 2019. BROWN was arrested on February 26, 2019 and interviewed by law enforcement agents. BROWN stated, in sum and substance and in part, that during different periods of the scheme, which he said lasted from 2015 to early 2017, he and ANDRE WILBURN split the profits from the sales of eVouchers

¹ Telegram and WhatsApp are two different cloud-based instant messaging and voice over IP services.

in cash and using SQC and that a Simple Bank account was used to hold cash that was sent to WILBURN via SQC. BROWN further stated that he communicated with WILBURN about eVoucher sales via Telegram and WhatsApp.²

17. LAMONT BROWN appeared before The Honorable Steven Tiscione, Magistrate Judge for the Eastern District of New York on February 26, 2019. Magistrate Judge Tiscione set bond in the amount of \$100,000 with certain conditions, including the monitoring of any internet-capable devices by Pretrial Services to ensure that BROWN.

18. On February 27, 2019, two officers from Pretrial Services (the “PSOs”) conducted an initial assessment of the residence of LAMONT BROWN. The PSOs advised BROWN that while he was released on bond, he was prohibited from using any internet-capable electronic devices without allowing Pretrial Services to first install monitoring software. BROWN provided the PSOs with a number of internet-capable devices, including the Device, and stated that the Device belonged to him.

19. On or about February 28, 2019, LAMONT BROWN reported to Pretrial Services as directed and asked if the Device could be returned to him. BROWN was advised that the Device would be returned to him after an officer from Pretrial Services reviewed the data on the Device and installed an “app lock.” An app lock is a security tool that can prevent someone from using certain applications, such as a web browser, without a password, and is used by Pretrial Services to monitor a defendant’s compliance with the conditions of his or her bond.

² Telegram and WhatsApp are two different cloud-based instant messaging and voice over IP services.

20. On or about March 5, 2019, a PSO examined the Device for the reasons explained above. The PSO observed an image of an Amtrak ticket bearing reservation number 637952 for passenger Lamont White to travel on October 23, 2017 to New York, Penn Station from Philadelphia, 30th Street Station. The PSO also observed an image of a computer screen showing an Amtrak itinerary for round-trip travel from New York, Penn Station to Washington, DC, Union Station. The PSO took photographs of these images and shared her findings and photographs with one of the law enforcement agents from HSI investigating the above-described fraudulent scheme.

21. I reviewed the photographs supplied by the PSO and determined that Amtrak reservation number 637952 was purchased using an eVoucher that had originated from a purchase of an Amtrak reservation made on October 18, 2017, for \$1142.00 (the "Original Purchase"). The Original Purchase was cancelled and exchanged into four different eVouchers (the "Resulting eVouchers") at different times, on October 20, 2017, October 23, 2017, October 25, 2017 and November 21, 2017. The Resulting eVouchers from October 20, 2017 and October 25, 2017 were sold on eBay by LAMONT BROWN using eBay account "liphet715." The Resulting eVoucher from November 21, 2017 was used for a reservation in the name of Linda Wilburn, which is the name of the mother of ANDRE WILBURN. The Resulting eVoucher from October 23, 2017 was used for a reservation for two passengers named Andre Wallace and Lamont White, which, based upon my training and experience, I believe to be aliases for ANDRE WILBURN and LAMONT BROWN. The Original Purchase had been made using a credit card account number belonging to an individual who reported the Original Purchase as unauthorized.

22. The Device is currently in the possession of Pretrial Services in the Eastern District of New York. Pretrial Services has advised a special agent from HSI that the Device will be provided to HSI if authorized by a court order.

23. On or about March 15, 2019, an indictment was filed charging LAMONT BROWN, ADAM MICEK, KEVIN NELSON and ANDRE WILBURN for crimes in connection with the fraudulent scheme described above. (Cr. Dkt. 19-139). BROWN was specifically charged with one count of conspiracy to commit wire fraud and one count of wire fraud, in violation of Title 18, United States Code, Sections 1349 and 1343.

TECHNICAL TERMS

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing

and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected

to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

25. Based on my training and experience, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, and GPS navigation device, with access to the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

file (such as a paragraph that has been deleted from a word processing file).

Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

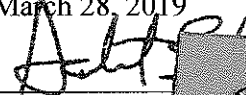
29. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

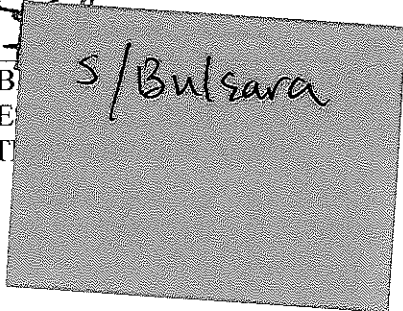
Respectfully submitted,



Christopher Carr
Special Agent
Amtrak, Office of Inspector General

Subscribed and sworn to before me
on March 28, 2019


THE HONORABLE
UNITED STATES
EASTERN DISTRICT OF



ATTACHMENT A

The property to be searched is a one ZTE Z861BL cellular phone bearing serial number 329F74220C07 (the “Device”). The Device is currently in the custody of Pretrial Services for the Eastern District of New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Titles 18, United States Code, Sections 1349 and 1343 (conspiracy to commit wire fraud and wire fraud), committed by LAMONT BROWN, together with others, from January 1, 2016 to the present, including:

- a. records and information relating to eBay, Craigslist and Amtrak;
- b. records and information relating to KEVIN NELSON, ADAM MICEK and ANDRE WILBURN;
- c. records and information relating to the transfer of money, including bank account information, credit card or Paypal information, and other methods of sending and receiving money, including but not limited to Square Cash; and
- d. financial records, including all bank records, checks, credit card bills.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.